Technical Cybersecurity

Bulb Protect!

We protect by stopping attackers at as many steps as possible.

Attack Process

Recon

- What versions of software?
- Known flaws?
- Can I access the vector?
- Default credentials?
- Easy credentials?
- What kind of traffic?
- Is the vector vulnerable?
- Is the vector exploitable?

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Defensive Techniques

Protect from recon

- *Hide version information!*
- *Don't use stuff with known exploits!*
- *Make vectors inaccessible!*
- *No default credentials!*
- *Strong credentials only!*
- *Encrypt traffic!*

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Attack Process

What can we do?

- We've checked out the system and we know what's there
- We have researched existing vulnerabilities and know if they're exploitable
- We have an idea how to exploit those
- Develop that idea into methods we can use to exploit

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Defensive Techniques

STOP ATTACKERS FROM DOING THINGS!

- *Make the system opaque!*
- *If you have no known vulnerabilities, you have no known exploits!*
- *Much more expensive to develop exploits from scratch*

Increase cost to exploit as much as possible!

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Attack Process

Trigger!

- Use the method to attack the actual device
- We want to get onto the device and then establish *persistence* (although not always needed)
- Trigger the exploit and install our code (or use the code that already exists)

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Defensive Techniques

Make comms hard

- *You've done your best, they may have found an exploit.*
- *Monitor for persistence*
- *Remove everything from your system that isn't absolutely needed*

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Attack Process

Do our thing

- So we now have some control over the device, we want to establish communication for Command & Control (C2)
- Escalate if needed

Repeat to further penetrate

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Defensive Techniques

Monitor for C2

- *Keep an eye on network traffic and look for anything out of place - IRC? odd information in HTTP headers? Large data flows?*
- *Harden the system internally to protect v. escalation - aim for no known vulnerabilities or exploits!*

Attack Surface

Vector 0: Bluetooth
Vector 1: HTTP Server
Vector 2: SSH Server
Vector 3: Misc Ports
Vector 4: DNS
Vector 5: HTTP Traffic
Vector 6: TCP/IP Traffic
Vector 7: Power Interface
Vector 8: Updates

Next: The Cyber Killchain